Eerste Kamer der Staten-Generaal 1

Vergaderjaar 2015–2016

34 353 EU-voorstel: Commissiemededeling inzake de overdracht van persoonsgegevens van de EU aan de VS naar aanleiding van het Schrems-arrest COM (2015) 566[1]

F BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 29 april 2016

Bijgaand treft u een afschrift aan van brief die ik heden aan de Voorzitter van de Tweede Kamer der Staten-Generaal zond.

De Minister van Veiligheid en Justitie,
G.A. van der Steur

[1] Zie dossier E150031 op www.europapoort.nl.

kst-34353-F
ISSN 0921 - 7371
’s-Gravenhage 2016

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 april 2016

Inleiding

In mijn brief van 16 februari 2016 (Kamerstukken II 2015/16, 32 317, nr. 388) zegde ik u toe een beoordeling te geven van het *EU – US Privacy Shield* zodra de teksten daarvan ter beschikking zijn gesteld. De Europese Commissie heeft deze teksten ter beschikking gesteld op 29 februari 2016. Bijgaand treft u deze teksten[2] aan. In het onderstaande voldoe ik aan de gedane toezegging. Ik merk daarbij op dat ook deze appreciatie berust op een eerste lezing van een omvangrijk en ingewikkeld pakket aan maatregelen en toezeggingen.

Leeswijzer

In het onderstaande ga ik eerst in op de structuur en het rechtskarakter van het EU – US Privacy Shield (hierna: Shield). Ik ga vervolgens kort in op de eigenlijke inhoud van het Shield, op het toezicht op de naleving en de handhaving ervan in de Verenigde Staten (VS), en daarna op de toegang door de overheid tot gegevens die met toepassing van het Shield worden doorgegeven en de daarbij geldende waarborgen voor de bescherming van de persoonlijke levenssfeer. Daarna geef ik een korte weergave van de voornaamste onderdelen van het advies van de Artikel 29 Werkgroep (WP 29) dat op 13 april 2016 is bekendgemaakt. Ik geef vervolgens een voorlopige beoordeling, waarbij ik het advies van WP 29 betrek. Ik sluit af met een schets van de procedure voor de vaststelling en het mogelijke vervolg daarvan.

Structuur en rechtskarakter EU – US Privacy Shield

Het Shield is formeel een ontwerpuitvoeringsbesluit van de Commissie gebaseerd op artikel 25, zesde lid, van richtlijn 95/46/EG (hierna: de richtlijn). Krachtens deze bepaling kan de Commissie constateren dat een derde land beschikt over een passend niveau van gegevensbescherming. Passend is een niveau dat in essentie gelijkwaardig is aan dat van de EU. Doorgaans bevatten dergelijke beslissingen een algemeen oordeel van de Commissie over het recht van het desbetreffende land. In dit geval is dit anders. Het gegevensbeschermingsrecht van de VS is zodanig verschillend van inhoud en opbouw van dat van de EU dat een dergelijk oordeel niet mogelijk lijkt. Het gegevensbeschermingsrecht heeft in de VS alleen een grondrechtelijke inbedding voor zover het de publieke sector betreft, terwijl het gegevensbeschermingsrecht in de private sector per deelgebied verschillend is opgebouwd en bovendien deels in andere instrumenten dan algemeen verbindende voorschriften is vastgelegd. Daarnaast ontbreekt een onafhankelijke toezichthouder op de verwerking van persoonsgegevens met een algemene bevoegdheid. Het ontwerpbesluit reflecteert de structuur van het gegevensbeschermingsrecht van de VS. Het is daarom alleen een oordeel over de passendheid van het gegevensbeschermingsniveau voor zover de desbetreffende sectoren daarin zijn betrokken. Die betrokkenheid is weer afhankelijk van de bevoegdheid van de toezichthouders met wie de Commissie afspraken heeft gemaakt. Dit zijn de *Federal Trade Commission* (FTC) en het *US Department of Transportation*. In heel grove trekken geschetst is de FTC bevoegd voor het toezicht op «fair trade» met inbegrip van gegevensbe-

[2] Ter inzage gelegd op de afdeling Inhoudelijke ondersteuning onder griffie nr. 159079.02.

schermingsaspecten op de private sector, met uitzondering van de financiële sector, de luchtvaartsector en de telecommunicatiesector. De luchtvaartsector valt onder de bevoegdheid van het *US Department of Transportation*. De financiële sector en de telecommunicatiesector en enkele andere sectoren vallen niet onder het Shield. Ik wijs erop dat het Shield bedoeld is om de doorgifte van persoonsgegevens uit de private sector in de EU naar de private sector in de VS te faciliteren. Zou het Shield niet bestaan, dan zullen bedrijven die persoonsgegevens aan de onder het Shield ingeschreven bedrijven doorgeven andere rechtsgrondslagen moeten gebruiken, zoals *Binding Corporate Rules* (BCR) (intern bindende bedrijfsvoorschriften vastgesteld op concernniveau) of door de Commissie goedgekeurde modelcontractsbepalingen (SCC's). Met het gebruik van deze instrumenten zijn doorgaans aanzienlijke kosten gemoeid. Die kosten zijn vooral voor het midden- en kleinbedrijf een relatief zware last. Het Shield kan niet worden gebruikt voor de doorgifte van gegevens uit de EU naar ontvangers uit de publieke sector in de VS.

Het ontwerpbesluit bevat 129 overwegingen waarin de Commissie omstandig motiveert waarom de VS onder toepassing van de voorwaarden en beperkingen van het Shield kunnen worden aangemerkt als een derde land met een passend niveau van gegevensbescherming. De artikelen van het ontwerpbesluit merken de VS daadwerkelijk als een zodanig derde land aan en geven functionele reikwijdte van het begrip «doorgifte» aan. Belangrijk is de verplichting van de Commissie om de relevante ontwikkelingen in de VS continu te monitoren. Een jaar na de datum van inwerkingtreding wordt de eerste evaluatie gehouden. Die zal voortaan jaarlijks gezamenlijk plaatsvinden. Er is voorzien in de verplichting de resultaten daarvan aan het relevante Comité, bestaande uit vertegenwoordigers van de lidstaten, en aan het Europees Parlement mee te delen. Verder is voorzien in een opschortingsbevoegdheid voor de Commissie.

Aan het ontwerpbesluit zijn zeven aanhangsels gehecht. Drie van die aanhangsels hebben zelf weer een aanhangsel. De meeste aanhangsels zijn «representations» (verklaringen en toezeggingen) van de bevoegde autoriteiten van de VS. Binnen 30 dagen na vaststelling van het besluit door de Commissie zal dit geheel van verklaringen in de VS in het *Federal Register* bekendgemaakt worden. Daardoor krijgen deze verklaringen een officieel karakter dat enigszins vergelijkbaar is met beleidsregels en richtlijnen in het Nederlands bestuursrecht.

Inwerkingtreding van het besluit heeft als rechtsgevolg dat persoonsgegevens met toepassing van de voorwaarden van het Shield zonder nadere garanties aan de bedrijven die zich onder het Shield hebben aangemeld kunnen worden doorgegeven. Het besluit laat alle andere rechtsgrondslagen voor de doorgifte van persoonsgegevens naar de VS onverlet. Het staat niet in de weg aan een doorgifte krachtens goedgekeurde SCC's of met toepassing van BCR's of aan welke andere rechtsgrondslag krachtens de artikelen 25 en 26 van de richtlijn dan ook.

Na inwerkingtreding van de Algemene verordening gegevensbescherming (hierna AVG) zal het besluit blijven gelden krachtens artikel 45, negende lid, van de AVG.

Inhoud EU – US Privacy Shield

De eigenlijke inhoud van het Shield is opgenomen in Annex II. Die inhoud bouwt in belangrijke mate voort op het Safe Harbour-arrangement. Daaraan zijn echter belangrijke formele en materiële verbeteringen toegevoegd. Formele verbeteringen zijn bereikt doordat de lijsten met

«Frequently Asked Questions» (FAQ's) uit het Safe Harbour-arrangement zijn omgezet in «Supplemental Principles», beginselen die aanvullend werken ten opzichte van de algemene beginselen van het Shield. De onduidelijke status van de FAQ's behoort daarmee tot het verleden. Het normatief gehalte van het Shield neemt daardoor toe. Op de materiële verbeteringen kom ik hieronder nog te spreken.

De hoofdbeginselen van het Safe Harbour-arrangement blijven ongewijzigd. Een bedrijf dat behoort tot een van de sectoren die wordt beheerst door de wetgeving waarvan de handhaving is opgedragen aan de FTC of het *US Department of Transportation* kan zich op basis van vrijwilligheid inschrijven bij het *US Department of Commerce* op de Privacy Shield website. Die inschrijving verplicht het bedrijf tot het naleven van zeven beginselen van gegevensbescherming. Het betreft:

«Notice» (bekendmakingsplicht over het eigen privacybeleid dat aan gedetailleerde eisen moet voldoen);

«Choice» (het op basis van opt out bieden van een keuzerecht aan betrokkenen over de verstrekking van gegevens aan derden of voor het gebruik van de gegevens voor een ander doel dan waarvoor ze zijn verzameld en het op basis van opt in bieden van dat keuzerecht waar het gevoelige gegevens betreft);

«Accountability for Onward Transfer» (de doorwerking van de Notice en Choice-beginselen voor gevallen van verstrekking aan derden);

«Security» (beveiligingsplicht);

«Data Integrity and Purpose Limitation» (doelbinding en instaan voor volledigheid en juistheid van de gegevens);

«Access» (rechten op inzage, verbetering en verwijdering van gegevens);

«Recourse, Enforcement and Liability» (verplichting tot bieden snelle, toegankelijke en onafhankelijke geschilbeslechtingsprocedures, verplichting tot informatieverschaffing aan het *Department of Commerce*, medewerkingsplicht aan een arbitragesysteem indien het klachtmechanisme niet tot oplossingen leidt, aansprakelijkheid).

Dit systeem wordt in de aanvullende beginselen overigens in vele details uitgewerkt. Het is niet goed mogelijk om daarvan in deze brief een volledig overzicht te geven.

Dit systeem van zelfregulering wordt aangevuld met overheidstoezicht door de FTC. Dit toezicht kan worden ingeroepen door belanghebbenden, hetzij rechtstreeks via een klacht, hetzij via een toezichthouder in de EU, die de klacht doorgeeft aan de FTC. De FTC heeft de mogelijkheid tot het opleggen van bestuurlijke boetes of het initiëren van strafvervolging bij schendingen van het Shield. Schendingen van het Shield worden door de FTC aangemerkt als schendingen van de geldende handelswetgeving («unfair trade practices»).

De Commissie heeft in haar Mededeling van 29 november 2013 (COM (2013) 847) (Kamerstukken II 2013/14, 22 112, nr. 1777) een reeks aanbevelingen gedaan over een verbetering van het toenmalige Safe Harbour-arrangement. Verreweg de meeste van deze aanbevelingen waren gericht op verduidelijking en verzwaring van de transparantieverplichtingen, op verbetering van de geschilbeslechtingsprocedures en op de handhaving van het aanmeldsysteem door het *US Department of Commerce*. De

materiële verbeteringen die het Shield biedt liggen hierin dat aan al deze aanbevelingen een bepaald gevolg is gegeven. Het komt erop neer dat het *US Department of Commerce* een aanmerkelijk striktere controle gaat uitvoeren op de juistheid en de actualiteit van de aanmeldingen – ook ambtshalve. Onjuiste of niet langer actuele beweringen van bedrijven over hun status onder het Shield worden gesanctioneerd. Verder zijn de voorwaarden voor verdere verwerking door derde partijen binnen de VS aangescherpt. Het hele systeem voor toezicht op de naleving en de handhaving is verstrekt. Ingeschreven bedrijven moeten klachten binnen 45 dagen behandelen. Het bestaande systeem voor alternatieve geschilbeslechting wordt kosteloos. Bij gevallen van onopgeloste klachten houden burgers uit de EU het recht bij de bevoegde toezichthouder een klacht in te dienen. Deze kan de zaak, afhankelijk van de aard van de klacht, aanmelden bij de FTC of het *Department of Commerce*. De FTC zal, hoewel daartoe krachtens de geldende wetgeving niet verplicht, deze klachten met voorrang in behandeling nemen. Als laatste optie voor de behandeling van onopgeloste klachten wordt een gezamenlijk Europees-Amerikaans «Privacy Shield Panel» opgericht. Dat panel kan een arbitraal vonnis vellen op grond van de *Federal Arbitration Act*. Dit is kosteloos afgezien van de kosten voor eventuele rechtsbijstand. Indien het arbitraal vonnis niet wordt gevolgd, is een procedure bij de federale rechter mogelijk. Een gang naar de rechter is ook zonder de tussenstap van arbitrage mogelijk. Kiest men ervoor naar de rechter te gaan dan zijn daaraan wel kosten verbonden.

Bedrijven kunnen er ook voor kiezen om op vrijwillige basis samen te werken met de bevoegde Europese toezichthouder. Het komt erop neer dat men dan bij klachten van burgers een onderzoek door een Europese toezichthouder aanvaardt en ook betrokkenheid van die instantie bij de geschiloplossing accepteert. Dit impliceert ook dat men een advies van de toezichthouder over de oplossing van de klacht of het geschil in beginsel opvolgt. Indien het bedrijf of de klager zich hiermee niet verenigt kan behandeling van de klacht aan een panel van Europese toezichthouders worden voorgelegd. Deze oplossingen impliceren overigens een principiële keuze voor de toepassing van EU-recht.

Toegang van de overheid tot doorgegeven gegevens

Annex II, § I.5, van het Shield formuleert dat binding aan de beginselen uit het Shield voor zoveel als noodzakelijk is («to the extent necessary») beperkt wordt als vereist is voor de nationale veiligheid, het openbaar belang en de rechtshandhaving. Het is deze beperking geweest die het Hof van Justitie van de EU (hierna: HvJEU) in de uitspraak van 6 oktober 2015, C-362/14 (Schrems), ertoe bracht na te gaan of de Safe Harbourbeschikking op die toegang wel voldoende beperkingen identificeerde en of daarbij wel voldoende waarborgen in acht genomen werden. Nu de Commissie daarbij in de eerdergenoemde Mededeling van 29 november 2013 had geconstateerd dat daarbij vragen konden worden gesteld, leidde die vaststelling tot de ongeldigverklaring van het besluit. Daaraan werd door het HvJEU toegevoegd dat de bij de toegang in acht te nemen maatstaf «strictly necessary and proportionate» behoort te zijn en dat betrokkenen moeten beschikken over een administratieve of rechterlijke middelen om de rechten op inzage, verbetering of verwijdering uit te oefenen. Het lag daarom op de weg van de Commissie een dergelijk onderzoek uit te voeren en daaraan zonodig consequenties te verbinden. In de overwegingen van het ontwerpbesluit doet de Commissie verslag van dit onderzoek. Dit heeft geleid tot diverse verklaringen van de autoriteiten in de VS waarin wordt geschetst hoe die toegang is georganiseerd en welke waarborgen daaraan zijn en worden verbonden. Die verklaringen betreffen de toegang van de autoriteiten in VS tot gegevens

die met toepassing van het Shield naar bedrijven in de VS zijn doorgegeven. Grondslagen in de wetgeving van de VS of mogelijkheden in de toepassingspraktijk om gegevens rechtstreeks in derde landen te vorderen of anderszins te verwerven vallen buiten de reikwijdte van het verrichte onderzoek. De onderlinge verstrekking van gegevens tussen autoriteiten in de EU en de VS zijn evenmin aan het onderzoek onderworpen.

Rechtshandhaving

Een afzonderlijke verklaring van het *US Department of Justice* (Annex VII) beschrijft de grondslagen die het Amerikaanse recht kent voor de toegang tot gegevens voor doeleinden verband houdend met de rechtshandhaving. Deze verklaring noemt een aantal hoofdcategorieën. Gemeenschappelijk kenmerk hiervan is dat deze bevoegdheden hetzij in opdracht van, hetzij onder toezicht van de rechter plaatsvinden in zaken met een strafrechtelijke achtergrond. Vorderingen tot het leveren van gegevens gericht tot individuen (of in de context van het Shield: bedrijven) kunnen blijkens de verklaring door de belanghebbende steeds worden aangevochten voor de bevoegde rechter.

Openbaar belang

Tenslotte geeft de verklaring van het *US Department of Justice* aan dat diverse toezichthoudende instanties beschikken over bevoegdheden om gegevens te vorderen bij bedrijven. Als voorbeeld worden de toezichthouders in financiële sector genoemd. Voor die gevallen moet steeds voorzien zijn in een wettelijke grondslag voor de vorderingsbevoegdheid en in toezicht door de rechter. Vorderingen kunnen door de belanghebbende bedrijven ook worden aangevochten.

Nationale veiligheid

De toegang tot gegevens wordt voor zover het gaat om «signals intelligence» (langs elektronische weg verworven inlichtingen) blijkens een omvangrijke verklaring van de *General Counsel* van het *Office of the Director of National Intelligence* (Annex VI) beheerst door het *Presidential Policy Directive 28* (hierna: PPD 28), vastgesteld door de President op 17 januari 2014. PPD 28 bevat algemene beleidsuitgangspunten die bij de uitoefening van wettelijke bevoegdheden tot het vergaren van persoonsgegevens in acht moeten worden genomen. Daarbij hoort dat de VS alleen persoonsgegevens verzamelen op een geldende rechtsgrondslag, met inachtneming van de beginselen van gegevensbescherming en burgerlijke vrijheden en voor rechtmatig vastgestelde doeleinden. Persoonsgegevens worden niet verzameld met het doel om kritiek of afwijkende meningen te onderdrukken of individuen te benadelen vanwege etniciteit, geslacht, seksuele oriëntatie of godsdienstige overtuiging. Er wordt ook geen onderscheid gemaakt in gegevens die wel en die niet betrekking hebben op Amerikaanse burgers. Evenmin, zo verklaart PPD 28, worden de bevoegdheden gebruikt ter bevordering van mededingingsvoordelen voor ondernemingen of sectoren van het Amerikaans bedrijfsleven.

Kern van de zaak is dat de vergaring van persoonsgegevens altijd plaatsvindt volgens de maatstaf «tailored as feasible». Dit betekent dat wanneer verzameling van persoonsgegevens plaatsvindt doelgerichte verzameling de voorkeur geniet boven verzameling in bulk. Dat betreft zowel de wijze van verzameling als de aard van de gegevens. Bij de keuze van de vormen van verzameling moet een afweging worden gemaakt tussen verschillende methoden. Bij de gegevens die het betreft moeten methoden worden toegepast als doelgerichte zoektermen. Ondanks deze

prioriteitsstelling kan verzameling van gegevens in bulk niet geheel worden gemist. Men verklaart echter bij die vergaringsmethode ook steeds gebonden te zijn aan de maatstaf «reasonableness». Volgens de verklaring impliceert dit een belangenafweging tussen doeleinden enerzijds en privacy en burgerlijke vrijheden anderzijds. Die doeleinden zijn beperkt tot: bedreigende activiteiten van vreemde mogendheden, bestrijding van terrorisme, maatregelen tegen proliferatie, cybersecurity, bedreigingen gericht tegen de eigen en bondgenootschappelijke krijgsmachten en de bestrijding van grensoverschrijdende criminaliteit, met inbegrip van het ontduiken van internationale sanctiemaatregelen. Het systeem wordt meer in detail beperkt door bepaalde planningsmethoden uiteengezet in de verklaring. Toezicht is primair intern georganiseerd en vindt plaats via «compliance officers» en een wettelijke gereguleerde *Inspector General* die elke dienst heeft. Deze functionaris adviseert en rapporteert in het openbaar aan het Congres. Een aanvullende vorm van toezicht die achteraf werkt is de onafhankelijke *Privacy and Civil Liberties Oversight Board* (PCLOB). Goedkeuring voor de toepassing van bepaalde bevoegdheden moet worden verkregen van het *Foreign Intelligence Surveillance Court* (FISC), een hof samengesteld uit federale rechters. Daarnaast is er een stelsel van politieke controle op de inlichtingendiensten.

De verzameling van persoonsgegevens vindt blijkens de verklaringen doorgaans plaats op grond van *Section* 702 van de *Foreign Intelligences Surveillance Act* (FISA). Kern van de verklaring is dat de vergaring van inlichtingen plaatsvindt met toepassing van «targeting» en «minimization» procedures. Verzameling in bulk vindt niet met toepassing van *Section* 702 plaats. Dit alles wordt getoetst door het FISC. De algemene beginselen van PPD 28 zijn daarop van toepassing. Het hierboven beschreven stelsel van privacywaarborgen eveneens. Een andere grondslag voor inlichtingenvergaring is de *USA FREEDOM Act*, vastgesteld in 2015 met het doel meer waarborgen voor de bescherming van de persoonlijke levenssfeer te bieden. Deze wet verbiedt de vergaring van verkeersgegevens verzameld door de telecommunicatiesector in bulk door de diverse autoriteiten. Blijkens de verklaringen moet de toepassing van de bevoegdheden door de autoriteiten op grond van de *USA FREEDOM Act* zo specifiek mogelijk plaatsvinden. De wet heeft ook de procedurele waarborgen voor het FISC verruimd door de mogelijkheid van amicus curiae brieven of hoorzittingen open te stellen voor, onder meer, behartigers van privacybelangen.

Daarnaast bieden de verklaringen nog inzicht in een groot aantal zeer uiteenlopende transparantieverplichtingen van overheid en bedrijfsleven. Ik meld hier in het bijzonder dat voorzien is in de mogelijkheid dat bedrijven mogen rapporteren over het aantal vorderingen tot het verstrekken van gegevens, al is dit door het hanteren van een afrondingsfactor beperkt tot een geaggregeerd niveau.

Ombudspersoon

De toepassing van bevoegdheden tot het vorderen van gegevens voor doeleinden verband houdend met de nationale veiligheid voorziet blijkens de verklaringen in de Annexen VI en VII in veel gevallen in een vorm van rechtsbescherming in de VS voor het bedrijf dat in de VS de desbetreffende gegevens heeft ontvangen krachtens het Shield. Aan de persoon op wie de gegevens betrekking heeft komt alleen dezelfde mate van rechtsbescherming toe wanneer voldaan kan worden aan het vereiste van belanghebbendheid. Dit kan bij de toepassing van sommige wetten problematisch zijn. Wanneer niet expliciet rechtsbescherming is opengesteld zonder onderscheid naar nationaliteit, stuit toegang tot de rechter

soms af op de vaste uitleg van het Vierde Amendement van de Amerikaanse Grondwet dat in de jurisprudentie en de praktijk zodanig wordt uitgelegd dat het de rechten beschermt van Amerikaanse burgers en degenen die rechtmatig hoofdverblijf houden in de VS. Om in een vorm van aanvullende rechtsbescherming te voorzien biedt de Amerikaanse regering de instelling van een Ombudspersoon aan (Annex III, verklaring van de *Secretary of State*). Die Ombudspersoon kan klachten op individueel niveau van betrokkenen in behandeling nemen, zonder onderscheid naar nationaliteit. De Ombudspersoon die zal worden ondergebracht bij het *US Department of State* kan na contact met de desbetreffende dienst beoordelen of de toepassing van de bevoegdheid waarover wordt geklaagd in overeenstemming plaatsvond met de geldende regelgeving en de wijze waarop die in Annex VI uiteengezet is. De Ombudspersoon is onafhankelijk van de inlichtingen- en veiligheidsdiensten. Toegang tot de Ombudspersoon is indirect. Net als bij het verdrag tussen de EU en de VS inzake het *Terrorist Finance Tracking System* vindt een voorafgaande toets plaats door een instantie in de lidstaat die moet beoordelen of de klacht voldoet aan de formele vereisten van de Annex. Wat Nederland betreft is middeling door een nog nader aan te wijzen overheidsorgaan nodig.

Belangrijk is dat besloten is het klachtrecht niet te beperken tot de toegang door de autoriteiten tot gegevens die krachtens het Shield zijn doorgegeven, maar ook krachtens de SCC's, BCR's of andere afwijkingen van de regel dat doorgifte alleen mag plaatsvinden naar staten ten aanzien waarvan een toereikendheidsoordeel is gegeven. Dat betreft ook afwijkingen op grond van de komende Algemene verordening gegevensbescherming.

Evaluatie, opschorting of intrekking

Een belangrijk onderdeel van het Shield is dat jaarlijks een evaluatie plaatsvindt. Die evaluatie vindt plaats met betrokkenheid van Europese toezichthouders en de Amerikaanse Ombudspersoon. Belanghebbenden uit het bedrijfsleven en van niet gouvernementele organisaties zullen door de Commissie op conferenties worden gehoord. Als het nodig is kan de Commissie de werking van de beschikking opschorten of desnoods intrekken. De Verenigde Staten zouden in theorie ook hun binding aan de verklaringen kunnen beëindigen. Het besluit wordt dan inhoudsloos. Intrekking wordt dan onvermijdelijk.

Advies Artikel 29 Werkgroep

De WP 29 (een onafhankelijke werkgroep bestaande uit vertegenwoordigers van de gegevensbeschermingstoezichthouders van de lidstaten, de Europees Toezichthouder voor Gegevensbescherming en de Commissie) heeft op 13 april 2016 zijn advies op het ontwerpbesluit vastgesteld (*Opinion 01/2016 on the EU-US Privacy Shield draft adequacy decision WP 238*). Gelijktijdig heeft WP 29 een document over essentiële Europese waarborgen voor de privacy en de bescherming van persoonsgegevens die in acht zouden moeten worden genomen wanneer met «surveillance measures» inbreuken op persoonsgegevens gemaakt die het voorwerp van doorgifte aan derde landen zijn (*Working Document 01/2016 on the justification of interferences with the fundamental right to privacy and data protection through surveillance measures when transferring personal data*, WP 237). WP 29 heeft een advies opgesteld dat in vier onderdelen te onderscheiden valt.

Het eerste onderdeel bevat enkele algemene opmerkingen. WP 29 verwelkomt de belangrijke inhoudelijke verbeteringen die het Shield ten opzichte van het Safe Harbour-arrangement brengt. WP 29 heeft echter

kritiek op de ingewikkelde structuur van het Shield. Omdat de uitgangspunten en waarborgen deels in het ontwerpbesluit en deels in de aanhangsels staan, zou de nodige informatie moeilijk te vinden zijn en op onderdelen ook innerlijk inconsistent. WP 29 wijst op de noodzaak om een met het geldend en komend EU-recht consistent Shield op te stellen. Bij inwerkingtreding van de AVG zou daarom een evaluatie moeten worden gehouden.

Het tweede onderdeel gaat in op de inhoudelijke aspecten van het Shield. WP 29 meent dat uit het «Data Integrity and Purpose Limitation Principle» onvoldoende duidelijk af te leiden valt of er een begrenzing aan het bewaren van gegevens bestaat en dat dit beginsel ook overigens onvoldoende bepaald is. Verder mist men een behandeling van de rechtsgevolgen van het nemen van geheel geautomatiseerde beslissingen. Ook acht WP 29 dat bij de gevolgen van verdere doorgifte uit de VS naar andere derde landen onvoldoende verzekerd is dat het beschermingsniveau van het Shield behouden blijft. Het stelsel van rechtsbescherming en geschiloplossing beoordeelt men als mogelijk te ingewikkeld in de praktijk.

Het derde onderdeel betreft de toegang van de overheid van de VS tot de doorgegeven gegevens om doeleinden die verband houden met de rechtshandhaving, andere openbare belangen en de nationale veiligheid. De afgelegde verklaringen van de autoriteiten van de VS beoordeelt WP 29 op zichzelf genomen als positief. Wat betreft de toegang voor doeleinden verband houdend met de rechtshandhaving en andere openbare belangen oordeelt men de uitleg van wettelijke grondslagen in Annex VII nogal beperkt in verhouding tot de complexiteit van de materie, het toezicht acht men voldoende robuust, maar men oordeelt de geboden rechtsbescherming onvoldoende, omdat de *Judicial Redress Act* – die regelt dat burgers van de lidstaten in hun hoedanigheid van betrokkenen in het gegevensbeschermingsrecht in rechte verhaal kunnen halen in de VS – geen einde maakt aan de situatie dat niet-Amerikanen zich niet rechtstreeks in rechte kunnen verzetten tegen bevelen tot het vorderen van gegevens. Wat betreft de toegang tot de doorgegeven gegevens voor doeleinden verband houdend met de nationale veiligheid is het oordeel negatief. WP 29 acht de mogelijkheid tot het massaal en ongericht verzamelen van gegevens van individuele burgers nooit proportioneel en strikt noodzakelijk in een democratische samenleving zoals de toepasselijke grondrechten vereisen. Alomvattend toezicht daarop acht WP 29 ook een vereiste. Wat de rechtsbescherming betreft vreest WP 29 dat de Ombudspersoon niet voldoende onafhankelijk is en niet over toereikende bevoegdheden beschikt om effectief toezicht te kunnen houden.

Het vierde onderdeel betreft de periodieke evaluatie, waaraan ook de nationale toezichthouders zullen deelnemen. Hierover is WP 29 in grote lijnen positief. Wel acht men het nodig de voorwaarden waaronder de evaluatie zal plaatsvinden, en de gevolgen die daaraan kunnen worden verbonden te verhelderen.

Dit waardevolle en op onderdelen ook wel kritische advies zal ik in mijn beoordeling betrekken voor zover het de hoofdlijnen betreft.

Beoordeling

Vergeleken met andere toereikendheidsoordelen op grond van artikel 25, zesde lid, van de richtlijn blijft het Shield, net als het Safe Harbour-arrangement, een bijzondere constructie. Het Shield is geen algemeen oordeel over de toereikendheid van het niveau van gegevensbescherming in de VS als geheel. De reikwijdte van het Shield is beperkt tot bedrijven

uit een aantal sectoren voor zover die zich bereid hebben verklaard het Shield te aanvaarden. In de VS bestaat geen algemeen bevoegde toezichthouder die specifiek is belast met het toezicht op de bescherming van persoonsgegevens. Deze omstandigheden zijn bij de onderhandelingen over het Shield door de Commissie als uitgangspunt gehanteerd. Men heeft moeten vaststellen dat het voor de VS geen optie was veranderingen in de wetgeving aan te brengen. Het Shield is daarom een systeem dat enerzijds zoveel mogelijk moet faciliteren dat gegevens die uit de EU afkomstig zijn zoveel mogelijk onderworpen blijven aan het beschermingsniveau van de EU en anderzijds ook voldoende verenigbaar zijn met het fundamenteel andere stelsel van gegevensbeschermingsrecht dat in de VS bestaat. De uitspraak van het HvJEU geeft in rechtsoverweging 81 in beginsel voldoende ruimte voor een toereikendheidsoordeel dat in de kern berust op zelfregulering, aangevuld met toezicht van overheidswege.

De opmerkingen in het advies van WP 29 over de structuur van het Shield, over de interne consistentie en de consistentie van het Shield met geldend en komend EU-recht lijken mij op zichzelf genomen terecht. De structuur van het Shield is ingewikkeld, al zie ik ook verbeteringen in de voorgestelde structuur ten opzichte van het Safe Harbour-arrangement. Uit die structuur vloeien nadelen voort die tot op zekere hoogte onvermijdelijk zijn. De opmerkingen van WP 29 over het consistent gebruik van de terminologie en het uitleggen van Amerikaansrechtelijke begrippen die afwijken van het EU-recht moet de Commissie ter harte nemen. Ik ga ervan uit dat de Commissie dit eigener beweging doet. Wat de samenhang tussen het Shield en de AVG betreft, is het voor de hand liggend dat de eerste evaluatie van het Shield de beste gelegenheid is voor een toets aan de AVG. De eerste evaluatie vindt blijkens artikel 4, vierde lid, van het ontwerpbesluit een jaar na de datum van bekendmaking van het besluit plaats.

Waar het gaat om het geven van opvolging aan de aanbevelingen van de Commissie uit november 2013 ben ik van oordeel dat de aanbevelingen met betrekking tot transparantie, toezicht op de naleving, handhaving, geschilbeslechting en aansprakelijkheid belangrijke verbeteringen van het stelsel van Safe Harbour zijn bereikt, terwijl tegelijkertijd het goede dat dit stelsel te bieden had behouden is gebleven. Dat draagt naar mijn mening bij aan een oordeel dat de VS voor de doorgiften die beheerst worden door het Shield een voldoende toereikend niveau van bescherming kunnen bieden.

Ik zie in elk geval een belangrijke verbetering in de nieuwe inspanningen die het *US Department of Commerce* op zich heeft genomen om in het vervolg een actieve rol te vervullen bij de inschrijving van bedrijven en het actueel houden van de inschrijvingen, alsmede op het actueel houden van de afgelegde privacyverklaringen door bedrijven. Eveneens merk ik als verbetering aan dat bedrijven door middel van een getrapt verlopend stelsel van klachtbehandeling verplicht worden om klachten van burgers op serieuze wijze te behandelen. De mogelijkheid om daarvoor uiteindelijk via arbitrage een oplossing te vinden waarborgt dat een neutrale en betaalbare wijze van klachtbehandeling kan plaatsvinden. Ik zie in het bijzonder in de mogelijkheid om de afdoening van klachten met betrokkenheid van Europese toezichthouders en met toepassing van EU-recht een grote stap voorwaarts. Verbetering zie ook in de toezegging van de *Federal Trade Commission* om de handhavingsinspanningen op een verder verhoogd niveau te brengen.

Er blijven verschillen bestaan tussen het Amerikaanse en het Europese recht. Gegevensbescherming wordt in het Amerikaanse recht niet als een

grondrecht aangemerkt, althans voor zover het betreft de private sector. Het toezicht en de rechtsbescherming zijn anders opgezet dan in de EU. Dat werkt door in de materiële normen. Die verschillen op onderdelen van het EU-recht. Met name het «Choice»-beginsel biedt bedrijven meer ruimte in hun verhouding tot consumenten dan in de EU het geval is. Dat betreft vooral het gebruik van gegevens voor andere doelen dan die waarvoor ze oorspronkelijk zijn verzameld, zoals direct marketing-doeleinden. Die verschillen zullen moeten worden aanvaard. Zij maakten deel uit van het Safe Harbour-arrangement en blijven onder het Shield bestaan. Het Europees bedrijfsleven is zich van dit verschil in concurrentiepositie bewust, is mij gebleken. Het bedrijfsleven blijkt echter zeer veel waarde te hechten aan de beëindiging van de rechtsonzekerheid die begonnen is met de ongeldigverklaring van het Safe Harbour-arrangement.

WP 29 heeft in zijn advies gewezen op verschillende onduidelijkheden in de betekenis van het «Data Integrity and Purpose Limitation Principle». Ik wil hier niet inhoudelijk ingaan op de concrete uitleg van begrippen van het Shield omdat dit bij uitstek een taak van de toezichthouders en de rechter is. Ik wijs er slechts op dat Annex II van het Shield een weergave is van Amerikaans recht, en niet van EU-recht en dat uit het Hofarrest niet voortvloeit dat Amerikaans recht letterlijk gelijk moet zijn aan EU-recht. Als er verschillen zijn is het zinvol die verschillen niet te verzwijgen, maar juist te verduidelijken. WP 29 beveelt daartoe aan in een verklarende woordenlijst te voorzien. Mogelijk kan de Commissie daarin voorzien op een wijze die niet leidt tot vergroting van het aantal documenten. Wat de opmerkingen van WP 29 betreft over verdere doorgifte, heeft de Commissie er juist in de afgelopen jaren herhaalde malen op gewezen dat dit voor haar een van de belangrijkste punten betrof. De gedachte is altijd geweest dat persoonsgegevens afkomstig uit de EU gedurende en na de doorgifte aan de VS niet aan een duidelijk lager beschermingsniveau zouden worden blootgesteld teneinde omzeiling van het niveau van het EU-recht te voorkomen. De inspanningen van de Commissie zijn naar mijn oordeel duidelijk zichtbaar in het Shield. De voorwaarden waaronder «onward transfer» gerechtvaardigd is, zijn in vergelijking met het Safe Harbour-arrangement duidelijk verzwaard. Kern daarvan is dat de partij die onder het Shield is ingeschreven aansprakelijk blijft voor handhaving van het beschermingsniveau dat het Shield biedt bij en na een verdere doorgifte (§ I.3 van Annex II). Dit impliceert mijns inziens dat een partij zich ook een algemeen beeld moet vormen van het gegevensbeschermingsniveau van een derde land en waar nodig en mogelijk aanvullende waarborgen moet treffen. Ik acht dit een zinvolle uitbreiding van het beschermingsniveau en deel de kritiek van WP 29 dan ook niet zonder meer. Waar WP 29 opmerkt dat het mechanisme voor rechtsbescherming en geschilbeslechting ingewikkeld is, kan ik dit beamen. Aan verduidelijking van structuur en mogelijkheden van het stelsel wordt inmiddels iets gedaan. De Commissie zal een *flowchart* maken die de werking verduidelijkt. Dat het stelsel daardoor in de praktijk niet effectief zou zijn, zoals WP 29 stelt, is een oordeel dat zonder dat daar ervaring mee is opgedaan niet kan worden onderschreven. Die ervaring is tot dusverre zeer beperkt. Blijkens mededelingen van de Amerikaanse autoriteiten zijn er in de afgelopen 15 jaar onder het Safe Harbour-arrangement slechts vijf klachten in het geschillenmechanisme behandeld. Wat ik belangrijk vind, is dat het stelsel is uitgebreid op een wijze die EU-burgers meer keuzes biedt.

Wat de bevoegdheden van de Amerikaanse overheid betreft tot de gegevens die onder het Shield zijn doorgegeven stel ik in de eerste plaats vast dat de VS in veel sterkere mate dan voorheen het geval was bereid zijn gebleken uit te leggen in welke gevallen toegang tot doorgegevens

gegevens kan worden verkregen, op welke grondslagen dit plaatsvindt en welke waarborgen daarbij in acht moeten worden genomen. Uit de verklaringen van de verschillende autoriteiten blijkt dat de desbetreffende bevoegdheden in de VS, anders dan wel wordt beweerd, wel degelijk zijn omgeven met voorzieningen gericht op het individualiseren en verengen van vorderingen. Ook kan in zijn algemeenheid niet worden beweerd dat bewaking van het privacyaspect bij toepassing niet of nauwelijks met waarborgen zou zijn omringd. Die waarborgen zijn er wel, al kennen de VS geen waarborgen in de vorm van onafhankelijke toezichthouders op gegevensbescherming naar Europees model. Het is ook niet zo dat er geen rechtsbescherming denkbaar is tegen de toepassing van de bevoegdheden. Ook die bestaat, al is die zeer divers opgezet en niet overal gelijkelijk toegankelijk voor eenieder onafhankelijk van hoedanigheid of belang.

Ik deel het algemene oordeel van WP 29 dat de uitgebreide verklaringen van de Amerikaanse autoriteiten tot verduidelijking van de bestaande grondslagen om toegang tot doorgegeven gegevens te verkrijgen voor doeleinden van de rechtshandhaving, andere openbare belangen of de nationale veiligheid sterk bijdragen aan transparantie van het rechtsstelsel in de VS en dat dit een betekenisvolle verbetering is ten opzichte van het Safe Harbour-arrangement.

Waar het gaat om toegang van de Amerikaanse overheid tot doorgegeven persoonsgegevens voor doeleinden die verband houden met de rechtshandhaving of om andere redenen van openbaar belang ben ik van mening dat uit de toezeggingen van het *US Department of Justice* (Annex VII) voortvloeit dat die toegang in voldoende mate op wet is gebaseerd. Bovendien zijn de bevoegdheden onderworpen aan verschillende soorten beleidsregels. Veelal geeft een voorafgaand oordeel van de rechter een aanvullende waarborg bij uitoefening van de bevoegdheden. Tegen een rechterlijk bevel is doorgaans een hogere voorziening mogelijk. Het betreft hier overigens steeds strafzaken of bestuursrechtelijke handhavingskwesties. In dit type zaken zullen in de regel alleen op het concrete geval gerichte vorderingen tot het leveren van gegevens worden gedaan.

WP 29 stelt in haar advies dat de wettelijke grondslagen voor de toegang tot gegevens voor doeleinden verband houdend met de rechtshandhaving en andere redenen van openbaar belang te weinig bestaan uit een min of meer volledige opsomming van die grondslagen en zich teveel concentreren op een beschrijving van de te volgen procedures. WP 29 meent onder verwijzing naar de uitspraak van het HvJEU in de dataretentiezaak (zaken C-293/12 en C-594/12) dan ook dat daardoor onvoldoende duidelijk is of noodzaak en proportionaliteit wel afdoende toetsbaar is, omdat dit niet goed mogelijk is wanneer die opsomming niet wordt gegeven. Hoewel het op het eerste gezicht niet onjuist lijkt dat Annex VII op onderdelen verschillende impliciete verwijzingen naar andere grondslagen bevat dan de grondslagen die wel expliciet zijn genoemd, kan ik niet beoordelen of Annex VII onvolledig is. Dat is zonder grondige kennis van het Amerikaanse systeem bovendien niet eenvoudig te beoordelen. Ik lees Annex VII zo dat de Amerikaanse overheid wil verduidelijken dat het Vierde Amendement van de Amerikaanse Grondwet rechtstreeks eist dat onmiddellijke ingrepen van de overheid in het huisrecht en het bezit van burgers, en ook over de zeggenschap over informatie, alleen zijn toegestaan als aan fundamentele procedurele waarborgen is voldaan, waaronder in elk geval voorafgaande beoordeling door een rechter. Inmenging in het recht dat in de EU als het grondrecht op bescherming van persoonsgegevens wordt aangemerkt van *andere* aard, zoals bijvoorbeeld de vordering van gegevens over de betrokkene *bij een derde*,

moeten krachtens genoemd Amendement tenminste voldoen aan de eis van «reasonableness», zo lees ik Annex VII. De grondslag voor dergelijke ingrepen, zo lees ik Annex VII, is te vinden in zeer uiteenlopende wettelijke voorschriften of federaal strafprocesrecht. Ik acht het bovendien niet buiten twijfel dat de eisen die het HvJEU in dit opzicht aan EU-recht stelt, zonder meer ook aan het recht van een derde land mogen worden tegengeworpen. «Essentially equivalent» betekent immers niet dat aan een derde land exact dezelfde maatstaven worden opgelegd als aan de Unie, maar dat het beschermingsniveau in essentie gelijkwaardig moet zijn. Er is ruimte voor een eigen invulling en ook voor een onderhandelingsmarge voor de Commissie. Die ruimte kan ook hierin bestaan dat men een meer procedureel georiënteerd recht op zijn eigen merites heeft beoordeeld en aanvaardt. Ik kan de Commissie in dit opzicht volgen. De rechtsbescherming tegen de desbetreffende bevoegdheden oordeelt WP 29 onvoldoende, onder meer omdat de het Vierde Amendement van de Amerikaanse Grondwet zodanig wordt uitgelegd dat de rechtsbescherming slechts kan worden ingeroepen door burgers van de VS en personen van andere nationaliteit die rechtmatig hoofdverblijf in de VS houden. Ik onthoud mij van een oordeel over de Grondwet van een derde land. Ik wijs er echter op dat de onderhandelingen plaatsvonden onder de vooronderstelling dat inzet van de onderhandelingen niet bestaat uit wijziging in de wetgeving van de VS. Wel is het zo dat met de totstandkoming van de *Judicial Redress Act* burgers van aangewezen staten hun rechten als betrokkene geldend zullen kunnen maken voor de Amerikaanse rechter. Deze stap staat formeel weliswaar los van het Shield, maar is daar wel nauw aan verbonden. Ik zie dit als een grote stap vooruit. Verder heb ik van de Amerikaanse autoriteiten begrepen dat ook al is er voor een EU-burger die geen hoofdverblijf in de VS houdt geen directe rechtsmiddel beschikbaar tegen vorderingen tot het leveren van gegevens die op hem betrekking hebben of die tot hem zijn gericht, het inroepen van bescherming op grond van andere wetgeving in de VS, zoals het equivalent van de openbaarheidswetgeving of een actie uit onrechtmatige overheidsdaad niet uitsluit.

De toegang van de autoriteiten van de VS tot de doorgegeven persoonsgegevens voor doeleinden verband houdend met de nationale veiligheid toont een uiteenlopend beeld. Ik acht het voldoende duidelijk dat met PPD 28 belangrijke hervormingen van het wettelijk stelsel voor het verzamelen van gegevens ten behoeve van de nationale veiligheid in gang zijn gezet. Die hervormingen leiden ertoe dat in elk geval op abstract niveau de veiligheidsbehoeften en de waarborgen voor de bescherming van de persoonlijke levenssfeer opnieuw tegen elkaar zijn afgewogen. Het is ook voldoende duidelijk dat het belang van de bescherming van de persoonlijke levenssfeer daarbij meer gewicht heeft gekregen. Waar het aankomt op de toepassing van concreet genoemde *Section* 702 FISA en de *USA FREEDOM Act* ben ik voldoende overtuigd door de verklaring dat de bevoegdheidsuitoefening als hoofdregel gericht plaatsvindt aan de hand van concrete zoekcriteria of persoonsgericht onderzoek. Er is sprake van voorafgaande toestemming door een rechter. De procedure vindt in camera en ex parte plaats, maar een recente aanpassing van het procesrecht voorziet in de mogelijkheid van aanstelling van een onafhankelijk raadsman die in zaken die zich daar volgens het FISC toe lenen advies te geven over de privacyaspecten van de zaak. Deze waarborg wordt aangevuld met andere waarborgen, vooral in de vorm van intern toezicht op de uitoefening van de bevoegdheid nadat de rechter de vordering heeft toegewezen.

Het is mij niet ontgaan dat PPD 28 de mogelijkheid openhoudt voor gegevensvergaring in bulk. Daarbij geldt wel dat dit niet de eerste optie is en dat de gegevens na verzameling aan de hand van goedgekeurde

criteria moeten worden beoordeeld. Ik wijs gegevensvergaring in bulk niet principieel van de hand om de enkele reden dat dit type vergaring plaatsvindt zonder onderscheid van personen. Ik acht gegevensvergaring in bulk een verantwoord middel voor de bescherming van de nationale veiligheid, indien er een noodzaak is dit middel in te zetten om gebeurtenissen als terroristische aanslagen en grote cyberaanvallen tegen te gaan. Naast een adequate toetsing van noodzakelijkheid en proportionaliteit van inzet van dit middel moeten daarbij dan wel de vereiste waarborgen voor de bescherming van de persoonlijke levenssfeer worden getroffen op een wijze die in essentie een gelijkwaardig beschermingsniveau bieden als in de EU geboden wordt. Ik ben mede tot dat oordeel gekomen, omdat de Europese wetgever met het politiek akkoord op de PNR-richtlijn immers ook een dergelijk systeem heeft aanvaard. Waar het dus op neerkomt is dat de verzamelde gegevens verder worden verwerkt op een wijze die met de nodige waarborgen is omringd. Deze waarborgen zijn opgesomd in Annex VI. De doeleinden waarvoor gegevensvergaring in bulk mag plaatsvinden zijn in elk geval voor een belangrijk deel herkenbaar en verwant aan de taken op grond waarvan de relevante Nederlandse wetgeving bevoegdheden toekent tot inmenging in het grondrecht van de bescherming van de persoonlijke levenssfeer voor doeleinden verband houdend met de nationale veiligheid. Ik ben ook van oordeel dat met de bekendmaking van PPD 28 en de diverse bronnen waarnaar in PPD 28 en Annex VI wordt verwezen een redelijk beeld wordt gegeven van de wettelijke en administratieve grondslagen voor die inmenging. Er zijn verschillende beperkingen bij de uitvoering weergegeven. Zo wordt de lijst van doeleinden jaarlijks opnieuw beoordeeld, en voor zoveel mogelijk ook openbaar gemaakt.

Gebruik van dit middel vindt plaats nadat de keuze daarvoor is beoordeeld op een hoger niveau binnen de administratie en waarbij expliciet de vraag aan de orde komt welke inbreuk op de bescherming van de persoonlijke levenssfeer met het voorgestelde middel gemoeid is. Er zijn verplichtingen vastgesteld om de vergaarde gegevens zoveel mogelijk aan de hand van concrete selectiecriteria als beoogde doelen (personen, groepen, telefoonnummers, plaatsen etc.) of onderwerpen (zoals proliferatie van massavernietigingswapens) te doorzoeken. Die beperkingen gelden ongeacht de nationaliteit of woonplaats van de betrokken personen. De interne toegang tot de gegevens is binnen de betrokken diensten verder beperkt. Ook bij de vergaring van gegevens in bulk is in intern toezicht in de vorm van een Inspector General en de PCLOB voorzien. Ik kan mij voorstellen dat deze voorzieningen de Commissie voldoende grond geven voor het oordeel dat bij deze gegevensvergaring aan de maatstaf «necessary and proportionate» die zij voor ogen had.

Zie ik het goed, dan kiest WP 29 voor een benadering die principieel anders is dan de bovengeschetste benadering. WP 29 wijst elke vorm van het massaal en ongericht verzamelen van gegevens van burgers van de hand, ongeacht of die verzameling onderworpen is aan waarborgen ter bescherming van de persoonlijke levenssfeer. Een onderscheid tussen verzamelen en gebruiken van gegevens en het koppelen van verschillende waarborgen aan de onderscheiden fasen van gegevensverwerking, zoals hierboven is weergegeven wijst WP 29 daarom eveneens van de hand. Ik respecteer dit standpunt, maar deel het niet. Ik ben van oordeel dat het wel zinvol kan zijn om de afweging tussen privacy en veiligheid verschillend te laten plaatsvinden al naar gelang het betreft het verzamelen, bewaren, gebruiken, verstrekken, doorgeven of vernietigen van gegevens. Op die afweging zijn tal van omstandigheden van invloed, zoals de aard van de gegevens, het aantal en de hoedanigheid van de betrokkenen, de bewaartermijnen, het mogelijk anonimiseren of pseudonimiseren van gegevens, de aard van partijen aan wie gegevens worden

verstrekt of doorgegeven, welke waarborgen bij verstrekken of doorgeven in acht moeten worden genomen, de feitelijke toegang tot de gegevens en de vernietiging ervan. Ik lees de ontwerpbeschikking zo de Commissie zich op vergelijkbare wijze heeft georiënteerd en daaraan een oordeel heeft verbonden. Een alomvattend toezicht op de verwerking van verzamelde gegevens acht WP 29 van belang. Ik leid hieruit af dat men het gelaagde stelsel van toezichtsmethoden in de VS niet voldoende acht. Het is echter zo dat de VS geen algemeen bevoegde toezichthouder voor gegevensbescherming kennen, ook niet in de context van de inlichtingen- en veiligheidsdiensten. Daarin zal moeten worden berust. Het is niet reëel te denken dat dit zal veranderen. Ook in Nederland is er sprake van een gelaagd toezicht op de inlichtingen- en veiligheidsdiensten met verschillende verantwoordelijkheden en bevoegdheden voor verschillende organen.

Wat de rechtsbescherming betreft, wordt in de verklaringen voldoende duidelijk uiteengezet dat betrokkenen, ongeacht hun nationaliteit, de bescherming door het FISC in te roepen tegen de uitoefening van bevoegdheid tot het vergaren van gegevens, mits zij in staat zijn hun individueel belang aan te tonen. Het nogal gecompliceerde stelsel van rechtsgrondslagen voor onderzoek biedt blijkens de verklaringen ook nog andere mogelijkheden van toegang tot de rechter, al lijkt die weg niet in alle gevallen open te staan.

Het is dan ook goed te zien dat VS duidelijk meer dan voorheen bereid zijn tegemoet te komen aan de Europese zorgen over het niet bestaan van een algemeen mechanisme in de VS om klachten van Europese burgers over de toegang van de autoriteiten tot doorgegeven gegevens te behandelen. Ik teken daarbij aan dat men ook besloten heeft de reikwijdte van het toezicht door de Ombudspersoon uit te breiden tot klachten die betrekking hebben op gegevens die zijn doorgegeven aan de VS krachtens andere grondslagen dan alleen het Shield. Er is nadrukkelijk gekeken naar alle krachtens de huidige richtlijn en de komende verordening in aanmerking komende grondslagen. De bij het *State Department* ingestelde Ombudspersoon kan die rol vervullen. Natuurlijk is de rol van een Ombudspersoon een andere dan die van de rechter. Daar moet wel bij worden bedacht dat ook in Nederland de Nationale ombudsman op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 bevoegd is om individuele klachten te behandelen tegen het optreden van de diensten en dat ook in Nederland geen rechtstreeks beroep op de bestuursrechter openstaat tegen besluiten van de bevoegde Ministers inzake de uitoefening van de door de wet in het leven geroepen bevoegdheden. Ik ben over deze stap van de VS dan ook positief.

WP 29 heeft duidelijke zorgen over de Ombudspersoon. Men betwijfelt of deze wel voldoende onafhankelijk is en of deze over voldoende bevoegdheden beschikt om effectief te kunnen zijn. Ik vind het van belang dat de Ombudspersoon door de positionering bij het State Department en de keuze van een hoog hiërarchisch niveau (onderminister) behoorlijke voorzieningen zijn om onafhankelijk van de inlichtingen- en veiligheidsdiensten te kunnen werken. Natuurlijk is een Ombudspersoon geen onafhankelijke rechter, maar dit staat onafhankelijk opereren niet per definitie in de weg. Ik wijs er ook op dat deze voorziening uniek is. Met geen enkel ander derde land – met inbegrip van alle derde landen die over een toereikendheidsoordeel beschikken – zijn tot dusverre vergelijkbare afspraken gemaakt. Ik heb dan ook met waardering kennis genomen van dit onderhandelingsresultaat.

Ik zie verder in het mechanisme voor de jaarlijkse evaluatie en de mogelijkheid van opschorting of intrekking een belangrijke stimulans voor

de Commissie om ervoor te zorgen dat de toezeggingen en verklaringen in het Shield steeds worden nagekomen en indien nodig ook worden besproken met de Verenigde Staten. Ik deel dan ook het oordeel van WP 29 dat dit mechanisme positief moet worden beoordeeld.

Al met al is mijn beoordeling van het geheel van het Shield overwegend positief. Ik kom daartoe omdat men zich op grond van aanmerkelijke inspanningen onder zeer hoge tijdsdruk de inhoud van de materiële normen heeft weten te verbeteren. Dat acht ik voor burgers én het bedrijfsleven van groot belang. Ik ben mij ervan bewust dat er bij de uitwerking van diverse onderdelen nog vragen zijn te stellen en nog wensen zijn te uiten. Ik realiseer mij daarbij ook dat de toegang van de overheid in de VS tot onder het Shield doorgegeven gegevens in veel gevallen mogelijk blijkt en dat de balans tussen privacy en veiligheid in Nederland op sommige vormen van toegang anders zou uitvallen. Er moet echter ook rekening worden gehouden met de omstandigheid dat een oordeel over ander rechtsstelsel een zeer gevoelige zaak is. Ik ben het dan ook met de Commissie en de VS eens dat dit geheel uitzicht biedt op een adequaat niveau van gegevensbescherming biedt aan doorgegeven gegevens. Ik denk wel dat het mogelijk is de overwegingen van het ontwerpbesluit verder te versterken. Een systematische opsomming van de criteria die in het arrest van het HvJEU zijn vastgesteld, gevolgd door een expliciete toets van het Shield, zou denkbaar zijn. De Commissie heeft aangegeven daarvoor open te staan, mits daarvoor bij de lidstaten een ruim voldoende draagvlak bestaat. Nederland zal beoordelen of het zich kan aansluiten bij voorstellen die door andere lidstaten in het vooruitzicht zijn gesteld. Ik zie, met inachtneming van deze marge voor een bescheiden verbetering, overigens ook geen goed alternatief voor het Shield.

Met hetgeen de Commissie heeft bereikt zijn naar mijn mening ook de aanbevelingen uit de meergenoemde Mededeling die betrekking hebben op de toegang van de overheid tot krachtens het Shield naar de VS doorgegeven gegevens van november 2013 opgevolgd. Ik ben er ook van overtuigd dat de zeer frequente evaluaties waartoe de ontwerpbeschikking verplicht, ertoe zullen leiden dat veel minder dan in de afgelopen 15 jaar het geval was een gevoel van zelfgenoegzaamheid over het geheel blijft bestaan en dat Commissie verplicht wordt om meer informatie met de lidstaten te delen.

Vaststelling

De procedure tot vaststelling van het besluit van de Commissie is geregeld in artikel 31 van de richtlijn. De Commissie raadpleegt de Europees Toezichthouder voor Gegevensbescherming krachtens verordening (EG) 45/2001. Dat advies is nog niet beschikbaar. Daarna vraagt de Commissie advies aan de Artikel 29 Werkgroep, bestaande uit de gegevensbeschermingstoezichthouders van de lidstaten. Op dat advies ging ik in het bovenstaande in. Vervolgens moet de Commissie advies vragen aan het Artikel 31 Comité dat bestaat uit vertegenwoordigers van de lidstaten. Daarna kan het besluit worden vastgesteld en bekendgemaakt. Dat comité vergadert op 29 april en 19 mei 2016. Na deze vergaderingen zal de Commissie het besluit vaststellen. Een uitvoeringsbesluit van de Commissie is krachtens artikel 263 VWEU vatbaar voor een vernietigingsberoep bij het HvJEU. Een dergelijk beroep kan worden ingediend door het EP, de Raad of door een lidstaat. De beroepstermijn is twee maanden na de datum van bekendmaking van het besluit in het Publicatieblad van de EU. Het is niet uitgesloten dat een dergelijk beroep wordt gedaan. Na inwerkingtreding is het besluit bindend voor de lidstaten en daarmee ook voor de toezichthouders die immers onderdeel

zijn van de lidstaten. Dat sluit echter niet uit dat de verenigbaarheid van het besluit met de artikelen 7 en 8 van het Handvest van de Grondrechten via een prejudiciële procedure volgend op een handhavingsactie in een lidstaat aan het HvJEU kan worden voorgelegd. Indien een nietigheidsberoep uitblijft is het is denkbaar dat dit zal gebeuren naar aanleiding van een nieuwe klacht bij een toezichthouder.

De Minister van Veiligheid en Justitie,
G.A. van der Steur